A FOURIER-ANALYTIC APPROACH TO COUNTING PARTIAL HADAMARD MATRICES

WARWICK DE LAUNEY AND DAVID A. LEVIN

ABSTRACT. In this paper, we study a family of lattice walks which are related to the Hadamard conjecture. There is a bijection between paths of these walks which originate and terminate at the origin and equivalence classes of partial Hadamard matrices. Therefore, the existence of partial Hadamard matrices can be proved by showing that there is positive probability of a random walk returning to the origin after a specified number of steps. Moreover, the number of these designs can be approximated by estimating the return probabilities. We use the inversion formula for the Fourier transform of the random walk to provide such estimates. We also include here an upper bound, derived by elementary methods, on the number of partial Hadamard.

1. Introduction

In this paper, we introduce a family of non-symmetric lattice random walks with importance to combinatorial design theory. Paths of these walks starting and ending at the origin correspond to partial Hadamard matrices (see below for the definition). These walks provide a tool for counting the number of partial Hadamard matrices, without recourse to the usual constructive methods adopted in design theory.

For non-negative integers n and t, a *partial Hadamard matrix* is an $n \times t$ matrix with ± 1 entries such that the inner product between any two distinct rows equals zero. Note that, since the rows of a partial Hadamard matrix D form a set of n independent t-dimensional real vectors, we must have $t \geq n$. Notice also that if we negate all the entries in a column of D, then the resulting matrix is also a partial Hadamard matrix. We say the two matrices are *column-negation equivalent*. Column-negation equivalence divides the set of $n \times t$ partial Hadamard matrices into equivalence classes of cardinality 2^t.

Date: March 23, 2010.

2000 *Mathematics Subject Classification.* 05B20, 15B10, 15B34, 60G50.

Key words and phrases. partial Hadamard matrices, random walks.

D.A.L. was partially supported by a Summer Research Award from the University of Oregon.

We now define our walk, and show that each distinct column-negation equivalence class of $n \times t$ partial Hadamard matrices corresponds to a distinct walk of length t terminating at 0. For an integer $n \geq 2$, set $d := \binom{n}{2}$, set $\mathbb{V}_m := \{-1, 1\}^m$, and let $Z : \mathbb{V}_n \to \mathbb{V}_d$ be defined by

$$Z(y) = (y_1 y_2, y_1 y_3, \dots, y_{n-1} y_n) , \tag{1}$$

so that the components of $Z(y)$ enumerate all pairwise products between the components of y. If $Y = [y^{(1)} \cdots y^{(t)}]$ is an $n \times t$ matrix with t column vectors $y^{(1)}, \dots, y^{(t)}$ belonging to $\mathbb{V}_n$, then

$$Z(y^{(1)}) + \cdots + Z(y^{(t)}) = 0$$

if and only if the inner product between any two rows of Y is zero.

Let

$$M := \{Z(y) \,:\, y \in \{-1, 1\}^n\} ,$$

then the map $Z : \mathbb{V}_n \to M$ is two-to-one, since $Z(-y) = Z(y)$. Indeed, the column-negation equivalence class of $n \times t$ partial Hadamard matrices

$$[\pm y^{(1)}, \pm y^{(2)}, \dots, \pm y^{(t)}]$$

maps to the single M-sequence

$$(m^{(1)}, m^{(2)}, \dots, m^{(t)}) = (Z(y^{(1)}), Z(y^{(2)}), \dots, Z(y^{(t)}))$$

of length t such that $\sum_i^t m^{(i)} = 0$. Thus, the number of $n \times t$ partial Hadamard matrices is equal to 2^{nt} times the probability that a random walk (X_t) with increments drawn uniformly from M returns to the origin.

We write $P_n^t(x, y)$ for the t-step transition matrix for (X_t):

$$P_n^t(x, y) := \mathbb{P}(X_t = y \mid X_0 = x) .$$

The random walk (X_t) has a number of unusual features. It has dimension $d = \binom{n}{2}$ but exponentially many (i.e., 2^{n-1}) possible increments, each with norm approximately $n/\sqrt{2}$. Thus, although, for n fixed, the usual functional central limit theorem applies (after proper rescaling of space and time, the walk converges in distribution to Brownian motion), the walk has special discrete structure which cannot be ignored. In particular,

- The support $\mathbb{L}_d$ of the walk, the smallest subgroup of $\mathbb{Z}^d$ containing M, is a strict subgroup of $\mathbb{Z}^d$,
- the walk has period 4, and
- the set of increments is non-symmetric.

Moreover, since there is no $n \times t$ partial Hadamard matrix for $t < n$ or $t \not\equiv 0 \pmod 4$, we must have $P_n^t(0, 0) = 0$ if either $t < n$ or $t \not\equiv 0 \pmod 4$. It is conjectured, but not proved, that the converse is true:

Conjecture 1. *For $n \geq 3$, $P_n^t(0,0) > 0$ if and only if $t \geq n$ and $t \equiv 0 \pmod 4$.*

This conjecture is equivalent to the Hadamard Conjecture, which asserts that there is a Hadamard matrix of order n for all n divisible by four. The following result is implied by recent work by de Launey and Gordon [3] and Graham and Shparlinski [4].

Theorem A. *For $\varepsilon > 0$ and all sufficiently large n, if $t - 2t^{\frac{113}{132}+\varepsilon} > 2n$ and $t \equiv 0 \pmod 4$, then $P_n^t(0,0) > 0$.*

Proof. Towards the end of their paper [4], Graham and Shparlinski note that the construction described in [3] applies without recourse to the Extended Riemann Hypothesis if one replaces the exponent 7/12 in Theorem Theorem 1.2 of [3] with the exponent 113/132. Thus for all sufficiently large n, there is an $n \times t$ partial Hadamard matrix whenever $n \leq \frac{t}{2} - t^{\frac{113}{132}+\varepsilon}$. ■

Thus, even before we begin our investigation of the walk (X_t), we know that there is a non-zero probability that our random walk returns to its start after about $2n$ steps. However, the proof depends on deep number-theoretic results concerning the existence of primes in short arithmetic sequences and special combinatorial constructions needed to prove the asymptotic existence of Hadamard matrices [2]. We hope that analytic techniques along the lines described in this paper will provide more direct proofs for theorems like Theorem A. Indeed, this paper contains a direct proof for the following result:

Theorem 1. *Let $\varepsilon > 0$. For all sufficiently large n, if $t \geq n^{12+\varepsilon}$ and $t \equiv 0 \pmod 4$, then $P_n^t(0,0) > 0$.*

This result is much weaker than Theorem A. However, the proof of Theorem 1 offers a number of advantages. Firstly, it generalizes to give results (which we derive elsewhere) for other kinds of designs such as balanced incomplete block designs and difference matrices.

Secondly, our analysis provides an accurate asymptotic formula for the number of distinct designs – a result which is not available even in the special case of partial Hadamard matrices. Specifically, for t large and n fixed, it is possible to prove a local central limit theorem for $P_n^t(0,0)$, yielding the following asymptotic formula for the number of partial Hadamard matrices:

Theorem 2. *Let $N_{n,t}$ be the number of partial Hadamard matrices of dimension $n \times t$, and let $d = \binom{n}{2}$. Then*

$$N_{n,4t} = [1 + o(1)] 2^{2d-n+nt+1} (8\pi t)^{-d/2} \quad \text{as } t \to \infty . \tag{2}$$

It should be emphasized that to apply the standard local limit theorem (e.g. [5, P9 on p. 79]) to our walk, we must first transform the walk so that, when sampled at multiples of 4, it is strongly aperiodic on $\mathbb{Z}^d$. However, as indicated above, the lattice $\mathbb{L}_d$ has a non-trivial structure, leading us to instead prove Theorem 2 directly from first principles. The proof uses the inversion formula (see, for example, [5, P3, p. 57])

$$P_n^t(0,0) = \frac{1}{(2\pi)^d} \int_{[-\pi,\pi]^d} \psi(\lambda)^t d\lambda\,, \tag{3}$$

where, for $\lambda \in \mathbb{R}^d$, the characteristic function $\psi(\lambda)$ is defined to be the expectation $\psi(\lambda) := 2^{-n+1} \sum_{x \in M} e^{\mathrm{i}\lambda \cdot x}$. Following the general approach outlined in [5], we observe that the dominant contribution to the integral on the right-hand side of (3) is from the neighborhoods of λ with $|\psi(\lambda)| = 1$. The number and deployment of these neighborhoods depends on the type of design being investigated. This paper gives a complete discussion of these neighborhoods for the walk corresponding to partial Hadamard matrices. This direct approach has the benefit of yielding error estimates in (2), and indeed these are strong enough to prove Theorem 1.

Thirdly, we obtain upper bounds for the number of partial Hadamard matrices. For example, we will prove the following theorem.

Theorem 3. *There are at most $2^{\binom{n+1}{2}}$ distinct Hadamard matrices of order n.*

Since there are precisely 2^{n^2} distinct $n \times n$ $(-1, 1)$-matrices, our result shows that the set of Hadamard matrices occupies at most about one square root of the entire search space. While our result is doubtless very weak, it shows that even for small orders being Hadamard is very rare.

It is worth pausing to emphasize that, when $t = n$, the integral on the right-hand side of (3) *exactly counts the number of Hadamard matrices*. Therefore, a positive resolution to the Hadamard conjecture is possible if it can be shown that this integral is positive. While we have not thus succeeded, we have been able to approximate the integral to obtain new results on the number of partial Hadamard matrices, and *we have done so without constructing a single design*. Thus the integral on the right-hand side of (3) might lead to a non-constructive proof of the Hadamard Conjecture. While we have left open the important (and probably difficult) problem of obtaining sharper estimates for the integral in equation (3) in the region close to $t = n$, this paper at the very least introduces an interesting non-symmetric lattice random

walk, where an understanding of the early (rather than the asymptotic) behavior of the transition probabilities for the walk is paramount.

The rest of this paper is organized as follows: In Section 2, we break up the integral on the right-hand side of (3) into manageable pieces. In Section 3, we obtain estimates on the characteristic function $\psi(\lambda)$. These estimates are used in Section 4 to obtain bounds on the return probabilities $P_n^t(0,0)$, from which Theorem 2 is derived. Theorem 1 is contained in Theorem 5.1. In Section 6, we prove Theorem 3, which is part of Corollary 6.3.

2. Anatomy of the Integral

In this section, we divide the region of integration for the integral

$$I(d,t) := \int_{[-\pi,\pi]^d} \psi(\lambda)^t d\lambda\,, \tag{4}$$

into manageable pieces.

We define the closed boxes

$$\mathrm{B}_\delta(\lambda) := \lambda + [-\delta,\delta]^d = \left\{\mu \in \mathbb{R}^d \;:\; \max_{1\le i<j\le n} |\mu_{\{i,j\}} - \lambda_{\{i,j\}}| \le \delta\right\},$$
$$\mathrm{B}_\delta := [-\delta,\delta]^d = \mathrm{B}_\delta(0)\,.$$

Let

$$\Lambda := \{\lambda \in \mathrm{B}_\pi \;:\; |\psi(\lambda)| = 1\}\,.$$

Since $0 \in \Lambda$, the set Λ is non-empty. Since, whenever $|\psi(\lambda)| < 1$, the magnitude of $\psi(\lambda)^t$ drops rapidly as t grows, it is natural to suppose that the bulk of the integral (4) is accounted for by points in B_π which are near an element of Λ. Consequently, we divide the region B_π of integration into the small pieces, $\{\mathrm{B}_\delta(\lambda) \;:\; \lambda \in \Lambda\}$, and the remaining piece

$$R_\delta := \mathrm{B}_\pi \setminus \bigcup_{\lambda\in\Lambda} \mathrm{B}_\delta(\lambda)\,. \tag{5}$$

We then estimate the integral (4) by combining our estimates for each of the pieces. The parameter $\delta \in (0,\pi/4)$ determines the sizes of the regions, and will be adjusted as needed.

Proposition 2.1. *For $\delta \in (0,\pi/4)$,*

$$I(n,4t) = 2^{2d-n+1}\int_{\mathrm{B}_\delta} \psi(\lambda)^{4t} d\lambda + \int_{R_\delta} \psi(\lambda)^{4t} d\lambda\,, \tag{6}$$

and, if $t \not\equiv 0 \pmod 4$, then $I(n,t) = \int_{R_\delta} \psi(\lambda)^t d\lambda$.

Proposition 2.1 will follow from the following two lemmas.

Lemma 2.2. *Let Λ be the set of λ with $|\psi(\lambda)| = 1$.*

(i) *If $\lambda \in \Lambda$, then $\psi(\lambda+\gamma) = \psi(\lambda)\psi(\gamma)$.*
(ii) *If*

$$\Lambda_0 := \{\lambda \in \mathbb{R}^d \,:\, \lambda_{\{i,j\}} \in \{0, \pm\pi/2, \pi\} \text{ for all } 1 \le i < j \le n\},$$

then $\Lambda \subset \Lambda_0$.

Remark 2.1. Notice that if $|\psi(\lambda)| = |\psi(\gamma)| = 1$, then Lemma 2.2(i) implies that $|\psi(\lambda+\gamma)| = 1$. In other words, Λ is closed under addition modulo 2π.

Lemma 2.3. *The multi-set $\{\psi(\lambda) \,:\, \lambda \in \Lambda\}$ contains exactly the elements $\pm 1, \pm i$, each appearing 2^{2d-n-1} times.*

We will prove Lemma 2.2 and Lemma 2.3 after deriving Proposition 2.1 from them.

Proof of Proposition 2.1. For $\delta < \pi/4$, by Lemma 2.2(ii), the boxes $\{\mathrm{B}_\delta(\lambda)\}_{\lambda\in\Lambda}$ are disjoint. Thus,

$$I(n,t) = \sum_{\lambda\in\Lambda} \int_{\mathrm{B}_\delta(\lambda)} \psi(\gamma)^t d\gamma + \int_{R_\delta} \psi(\gamma)^t d\gamma\,. \tag{7}$$

By Lemma 2.2(i), we have $\int_{\mathrm{B}_\delta(\lambda)} \psi(\gamma) d\gamma = \psi(\lambda) \int_{\mathrm{B}_\delta} \psi(\gamma) d\gamma$, which together with (7) shows that

$$I(n,t) = \sum_{\lambda\in\Lambda} \psi(\lambda) \int_{\mathrm{B}_\delta} \psi(\gamma) d\gamma + \int_{R_\delta} \psi(\gamma)^t d\gamma\,. \tag{8}$$

This identity together with Lemma 2.3 yield

$$\begin{aligned} I(n,t) = 2^{2d-n-1} \left[1^t + i^t + (-1)^t + (-i)^t\right] \int_{\mathrm{B}_\delta} \psi(\gamma)^t d\gamma \\ + \int_{R_\delta} \psi(\gamma)^t d\gamma\,. \end{aligned} \tag{9}$$

The sum $1^t + i^t + (-1)^t + (-i)^t$ vanishes unless $t \equiv 0 \pmod 4$, in which case it equals 4. This observation together with (9) finishes the proof. ∎

Proof of Lemma 2.2. We prove Part (i). First, observe that

$$\lambda \in \Lambda \qquad \Longleftrightarrow \qquad e^{\mathrm{i}\lambda\cdot Z(y)} = e^{\mathrm{i}\lambda\cdot Z(w)} \quad (\forall\, y, w \in \mathbb{V}_n)\,. \tag{10}$$

That is, if $\lambda \in \Lambda$, then $\psi(\lambda) = e^{i\lambda\cdot Z(y)}$ for all $y \in \mathbb{V}_n$. Consequently,

$$\psi(\lambda+\gamma) = 2^{-n} \sum_{y\in\mathbb{V}_n} e^{\mathrm{i}Z(y)\cdot(\lambda+\gamma)} = 2^{-n} \sum_{y\in\mathbb{V}_n} \psi(\lambda) e^{\mathrm{i}Z(y)\cdot\gamma} = \psi(\lambda)\psi(\gamma)\,.$$

Next, we prove Part (ii). The equations in the right-hand statement of the equivalence (10) are equivalent to the following system of modulo 2π linear equations:

$$\sum_{i<j} \lambda_{\{i,j\}} y_i y_j \equiv \sum_{i<j} \lambda_{\{i,j\}} w_i w_j \pmod{2\pi} \qquad (\forall\, y, w \in \mathbb{V}_n)\,. \tag{11}$$

Fix $\lambda \in \Lambda$. For $y \in \mathbb{V}_n$ and $k \in \{1, 2, \ldots, n\}$, define

$$\hat{y}_j^{(k)} = \begin{cases} \;\;\, y_j & \text{if } j \neq k, \\ -y_k & \text{if } j = k\,. \end{cases}$$

Taking $w = \hat{y}^{(k)}$ in (11) shows that

$$2 \sum_{i\,:\, i \neq k} \lambda_{\{i,k\}} y_i \equiv 0 \pmod{2\pi} \qquad (\forall k \in \{1, 2, \ldots, k\})\,. \tag{12}$$

Since this holds for any choice of $y \in \mathbb{V}_n$, it holds also for $\hat{y}^{(j)}$, whence we have the following two instances of (12):

$$2\lambda_{\{j,k\}} y_j + 2 \sum_{i\,:\, i \notin \{j,k\}} \lambda_{\{i,k\}} y_i \equiv 0 \pmod{2\pi}\,,$$

$$-2\lambda_{\{j,k\}} y_j + 2 \sum_{i\,:\, i \notin \{j,k\}} \lambda_{\{i,k\}} y_i \equiv 0 \pmod{2\pi}\,.$$

Therefore, for all $1 \leq j < k \leq n$, it follows that $4\lambda_{\{j,k\}} \equiv 0 \pmod{2\pi}$, that is, $\lambda_{\{j,k\}} \in \{0, \pm\pi/2, \pi\}$. ∎

From Lemma 2.2(ii), we know that $\Lambda \subset \Lambda_0$. In fact, this inclusion is strict. To prove Lemma 2.3, we need to characterize further the set Λ. In view of this, we introduce the following two sets: Let

$$\Lambda_1 = \{\lambda \in \mathbb{R}^d \,:\, \lambda_{\{i,j\}} \in \{0, \pi\} \text{ for all } 1 \leq i < j \leq n\}\,,$$

$$\Lambda_2 = \{\lambda \in \mathbb{R}^d \,:\, \lambda_{\{i,j\}} \in \{0, \pi/2\} \text{ for all } 1 \leq i < j \leq n\}\,.$$

These sets have several important properties. The set Λ_1 is closed under addition modulo 2π, and Λ_2 is closed under addition modulo π. Furthermore, $\Lambda_0 = \Lambda_1 + \Lambda_2$, meaning that every $\lambda^{(0)} \in \Lambda_0$ can be written in the form

$$\lambda^{(0)} \equiv \lambda^{(1)} + \lambda^{(2)} \pmod{2\pi}, \quad \text{where } \lambda^{(1)} \in \Lambda_1,\ \lambda^{(2)} \in \Lambda_2\,. \tag{13}$$

Moreover, because Λ_0 contains 4^d elements, and the sets Λ_1 and Λ_2 each contain 2^d elements, this representation is unique.

Recall, as noted in Remark 2.1, Λ is closed under addition modulo 2π. Notice that, since $e^{\pm\pi i} = -1$, the set Λ contains Λ_1. Therefore, the element $\lambda^{(0)} = \lambda^{(1)} + \lambda^{(2)}$ of Λ_0 is in Λ if and only if $\lambda^{(2)} \in \Lambda$. Consequently, if we define $\Lambda_2^\star = \Lambda \cap \Lambda_2$, then $\Lambda = \Lambda_1 + \Lambda_2^\star$. We will

now identify the set $\Lambda_2^\star$. Note that (13) implies that any $\lambda \in \Lambda$ can be written uniquely as

$$\lambda \equiv \lambda^{(1)} + \lambda^\star \pmod{2\pi}, \quad \text{where } \lambda^{(1)} \in \Lambda_1,\ \lambda^\star \in \Lambda_2^\star. \tag{14}$$

Each $\Lambda^{(2)} \in \Lambda_2$ has a combinatorial characterization. For each element $\lambda^{(2)} \in \Lambda_2$ we define a weighted graph G_λ on the vertices $\{1, 2, \ldots, n\}$ by including an edge $\{i, j\}$ if and only if $\lambda_{\{i,j\}} > 0$. We say a graph is *even-degree* if all of its vertices have even degree. We define

$$\Lambda_2^{\text{even}} = \{\lambda \in \Lambda_2 \,:\, G_\lambda \text{ is even-degree}\}.$$

We can now provide a useful characterization of the set $\Lambda^\star$.

Lemma 2.4. *We have* $\Lambda_2^\star = \Lambda_2^{\text{even}}$.

To prove Lemma 2.4, we will need to know that even-degree graphs are built-up from triangle graphs. We denote by $T_{\{a,b,c\}}$ the graph on the vertices $\{1, 2, \ldots, n\}$ with the edges $\{a, b\}, \{b, c\}, \{c, b\}$. Let G and H be graphs on the vertex set $\{1, 2, \ldots, n\}$. Then $G \oplus H$ is the graph with vertices $\{1, 2, \ldots, n\}$ which contains the edge $\{i, j\}$ if and only if $\{i, j\}$ is an edge of exactly one of G and H.

Lemma 2.5. *The set* Λ_2^{even} *consists of the elements* $\lambda \in \Lambda_2$ *such that* $G_\lambda = \oplus_{\{a,b,c\} \in \mathcal{T}_\lambda} T_{\{a,b,c\}}$ *for some set of triples* $\mathcal{T}_\lambda$.

Proof. We proceed by induction on the number E of edges. The statement is true for $E = 0$. There are no non-empty, even-degree graphs with fewer than three edges, and the only even-degree graph with three edges is a triangle. Thus, the claim is true for $E = 3$. Suppose now that it holds for all even-degree graphs with strictly fewer than $m > 0$ edges, and suppose that G_λ has m edges. Since G_λ has all degrees even, at least two edges, say $\{a, b\}$ and $\{a, c\}$, emanate from the same vertex, say a. So the mod 2 sum $G_\lambda \oplus T_{\{a,b,c\}}$ has strictly fewer than m edges, and, since $T_{\{a,b,c\}}$ has all even degrees, so does $G_\lambda \oplus T_{\{a,b,c\}}$. By the induction hypothesis, $G_\lambda \oplus T_{\{a,b,c\}}$ can be decomposed in triangles. Since $G_\lambda = (G_\lambda \oplus T_{\{a,b,c\}}) \oplus T_{\{a,b,c\}}$, it follows that G_λ also has such a decomposition. ■

Proof of Lemma 2.4. First, suppose $\lambda \in \Lambda_2^\star := \Lambda \cap \Lambda_2$. Then the equations (12) hold for all $k \in \{1, 2, \ldots, n\}$. Equation (12) holds for $k \in \{1, 2, \ldots, n\}$ if and only if $2\lambda_{\{i,k\}} = \pi$ for an even number of $i \in \{1, 2, \ldots, n\} \setminus \{k\}$. By definition of G_λ, this holds if and only if the degree of vertex k in the graph G_λ is even. Thus, G_λ is an even-degree graph, that is, $\lambda \in \Lambda_2^{\text{even}}$. Therefore, $\Lambda_2^\star \subset \Lambda_2^{\text{even}}$.

Next, suppose that $\lambda \in \Lambda_2^{\text{even}}$. By Lemma 2.5, there exists a set of triples $\mathcal{T}_\lambda$ such that

$$G_\lambda = \oplus_{\{a,b,c\} \in \mathcal{T}_\lambda} T_{\{a,b,c\}} \,.$$

Let $\lambda^{(\{a,b,c\})} \in \Lambda_2^{\text{even}}$ be defined as

$$\lambda^{(\{a,b,c\})}_{\{i,j\}} := \begin{cases} \frac{\pi}{2} & \text{if } \{i,j\} \subset \{a,b,c\}, \\ 0 & \text{otherwise} \,. \end{cases}$$

Then,

$$\lambda \equiv \sum_{\{a,b,c\} \in \mathcal{T}_\lambda} \lambda^{(\{a,b,c\})} \pmod{2\pi} \,.$$

Now, for all $y \in \mathbb{V}_n$,

$$\lambda^{(\{a,b,c\})} \cdot Z(y) = \tfrac{\pi}{2}(y_a y_b + y_a y_c + y_b y_c) \equiv -\tfrac{\pi}{2} \pmod{2\pi} \,. \tag{15}$$

Thus, for all $y \in \mathbb{V}_n$,

$$\lambda \cdot Z(y) \equiv -\frac{\pi}{2}|\mathcal{T}_\lambda| \pmod{2\pi} \,.$$

In particular, $e^{\mathrm{i}\lambda \cdot Z(y)} = e^{-\mathrm{i}\frac{\pi}{2}|\mathcal{T}_\lambda|}$, and is independent of y. Therefore, $\lambda \in \Lambda \cap \Lambda_2 =: \Lambda_2^\star$. We conclude that $\Lambda_2^{\text{even}} \subset \Lambda_2^\star$. ∎

Lemma 2.6. *The cardinality of Λ_2^{even} is $2^{\binom{n-1}{2}}$.*

Proof. Each graph with all degrees even on n vertices corresponds to a zero-diagonal $n \times n$ symmetric $(0,1)$-matrix all of whose rows and columns have even weight, and each such matrix corresponds to a unique zero-diagonal $(n-1) \times (n-1)$ symmetric $(0,1)$-matrix. Since there are exactly $2^{\binom{n-1}{2}}$ such matrices, we have $|\Lambda_2^{\text{even}}| = 2^{\binom{n-1}{2}}$. ∎

Proof of Lemma 2.3. By Lemma 2.6, the size of Λ_2^{even} equals 2^{d-n+1}. By (14), $|\Lambda| = 2^{2d-n+1}$.

Let $\mu = \lambda^{(\{a,b,c\})}$. By (15), $\psi(\mu) = -\mathrm{i}$. For all $\lambda \in \Lambda$, by Lemma 2.2(i), $\psi(\lambda + \mu) = -\mathrm{i}\psi(\lambda)$. Therefore, the multi-set $\{\psi(\lambda) : \lambda \in \Lambda\}$ has the composition as stated in the lemma. ∎

Proposition 2.1 leaves us with the problem of computing the integral of $\psi(\gamma)^{4t}$ over two regions: the *primary region* B_δ and the *secondary region* $R_\delta = \mathrm{B}_\pi \setminus \bigcup_{\lambda \in \Lambda} \mathrm{B}_\delta(\lambda)$. We conclude this section by dividing the secondary region R_δ into convenient pieces.

Lemma 2.7. *If Λ_2^{odd} is the set of the elements of Λ_2 whose associated graph has at least one odd degree, then*

$$R_\delta = \left[\bigcup_{\lambda \in \Lambda_1 + \Lambda_2^{\text{even}}} \mathrm{B}_{\frac{\pi}{4}}(\lambda) \setminus \mathrm{B}_\delta(\lambda) \right] \cup \left[\bigcup_{\lambda \in \Lambda_1 + \Lambda_2^{\text{odd}}} \mathrm{B}_{\frac{\pi}{4}}(\lambda) \right], \tag{16}$$

where the sets in the union are disjoint.

Proof. The unit circle can be divided up into four shifted pieces of length $\frac{\pi}{2}$ centered on the points $1, e^{\mathrm{i}\frac{\pi}{2}}, e^{-\mathrm{i}\frac{\pi}{2}}$, and $e^{\mathrm{i}\pi}$. Therefore, any $\gamma \in \mathrm{B}_\pi$ may be written uniquely in the form

$$\gamma \equiv \lambda(\gamma) + \delta(\gamma) \pmod{2\pi},$$

where $\delta(\gamma) \in \mathrm{B}_{\frac{\pi}{4}}$ and $\lambda(\gamma) \in \Lambda_0$. Thus

$$\mathrm{B}_\pi = \bigcup_{\lambda \in \Lambda_0} \mathrm{B}_{\frac{\pi}{4}}(\lambda),$$

and

$$R_\delta = \left[\bigcup_{\lambda \in \Lambda_0 \setminus \Lambda} \mathrm{B}_{\frac{\pi}{4}}(\lambda) \right] \cup \left[\bigcup_{\lambda \in \Lambda} \mathrm{B}_{\frac{\pi}{4}}(\lambda) \setminus \mathrm{B}_\delta(\lambda) \right]. \tag{17}$$

Recall that $\Lambda_0 = \Lambda_1 + \Lambda_2$, and $\Lambda_2 \cap \Lambda = \Lambda_2^{\mathrm{even}}$. Since $\Lambda_2 = \Lambda_2^{\mathrm{even}} \cup \Lambda_2^{\mathrm{odd}}$,

$$\Lambda_0 \setminus \Lambda = \Lambda_1 + \Lambda_2^{\mathrm{odd}} \quad \text{and} \quad \Lambda = \Lambda_1 + \Lambda_2^{\mathrm{even}}.$$

The identity (16) now follows from (17). ∎

In subsequent sections, we derive upper bounds for the integrals

$$\int_{\mathrm{B}_\rho(\lambda)} \psi(\gamma)^{4t} d\gamma$$

which depend only on whether λ is in $\Lambda_2^{\mathrm{even}}$ or Λ_2^{odd}.

3. Estimates for $\psi(\lambda)$

In this section, we obtain estimates for the magnitude, the real part, and the imaginary part of $\psi(\lambda)$. As a corollary, we obtain an upper bound for the integral over the secondary region.

Lemma 3.1. *The following bounds hold over the entire region* B_π*:*

$$|\psi(\lambda)|^2 \le \tfrac{1}{2} + \tfrac{1}{2} \prod_{i\,:\, i \ne k}^{n-1} \cos(2\lambda_{\{i,k\}}), \tag{18}$$

$$\mathrm{Re}(\psi(\lambda)) \ge 1 - \tfrac{1}{2}\|\lambda\|^2. \tag{19}$$

Suppose $\delta > 0$*, and that* $\lambda \in \mathrm{B}_\delta$*. Then*

$$\mathrm{Re}(\psi(\lambda)) = e^{-\frac{1}{2}\|\lambda\|^2}\bigl(1 + \varepsilon_1(\lambda)\bigr), \tag{20}$$

$$\mathrm{Im}(\psi(\lambda)) = -\sum_{i<j<k} \lambda_{\{i,j\}}\lambda_{\{j,k\}}\lambda_{\{k,i\}} + \varepsilon_2(\lambda), \tag{21}$$

where $|\varepsilon_1(\lambda)| < \frac{1}{12}(n\delta)^4 e^{\frac{1}{2}n^2\delta^2}$*, and* $|\varepsilon_2(\lambda)| < \frac{1}{12}(n\delta)^4$*.*

Proof. We first prove (18). Let $y \in \mathbb{V}_n$ and $\lambda \in \mathbb{R}^d$. For $i \in \{1, 2, \ldots, n\}$, define

$$\begin{aligned} p_i(\lambda) &= (\lambda_{\{1,i\}}, \lambda_{\{2,i\}}, \ldots, \lambda_{\{i-1,i\}}, \lambda_{\{i,i+1\}}, \ldots, \lambda_{\{i,n\}}) , \\ Z_i(y) &= (y_1, y_2, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n) , \\ P_i(\lambda) &= (\lambda_{\{j,k\}})_{1 \le j < k \le n,\, j,k \ne i} , \\ Q_i(y) &= (y_j y_k)_{1 \le j < k \le n,\, j,k \ne i} . \end{aligned}$$

Note that $p_i(\lambda)$ and $Z_i(y)$ are in $\mathbb{R}^{n-1}$, and $P_i(\lambda)$ and $Q_i(y)$ are in $\mathbb{R}^{d-n+1}$. Also, the maps p_i and P_i are linear. Recalling the definition of $Z(y)$ for $y \in \mathbb{V}_n$ in (1), observe that for all $i \in \{1, \ldots, n\}$,

$$Z(y) \cdot \lambda = p_i(\lambda) \cdot y_i Z_i(y) + P_i(\lambda) \cdot Q_i(y) .$$

For all $k \in \{1, 2, \cdots, n\}$,

$$\begin{aligned} \psi(\lambda) &= 2^{-n} \sum_{y \in \mathbb{V}_n} e^{\mathrm{i} p_k(\lambda) \cdot y_k Z_k(y)} e^{\mathrm{i} P_k(\lambda) \cdot Q_k(Z_k(y))} \\ &= 2^{1-n} \sum_{z \in \mathbb{V}_{n-1}} \tfrac{1}{2} \left[e^{\mathrm{i} p_k(\lambda) \cdot z} + e^{-\mathrm{i} p_k(\lambda) \cdot z} \right] e^{\mathrm{i} P_k(\lambda) \cdot Q_k(z)} . \end{aligned}$$

Therefore,

$$\begin{aligned} |\psi(\lambda)| &\le \frac{1}{2^{n-1}} \sum_{z \in \mathbb{V}_{n-1}} \tfrac{1}{2} \left| e^{\mathrm{i} p_k(\lambda) \cdot z} + e^{-\mathrm{i} p_k(\lambda) \cdot z} \right| \\ &= \frac{1}{2^{n-1}} \sum_{z \in \mathbb{V}_{n-1}} \left| \cos(p_k(\lambda) \cdot z) \right| . \end{aligned}$$

By Jensen's inequality,

$$|\psi(\lambda)|^2 \le 2^{-(n-1)} \sum_{z \in \mathbb{V}_{n-1}} \cos^2(p_k(\lambda) \cdot z) . \tag{22}$$

Since $2 \cos^2 \theta = 1 + \cos(2\theta)$,

$$|\psi(\lambda)|^2 \le \frac{1}{2} \left[1 + 2^{-(n-1)} \sum_{z \in \mathbb{V}_{n-1}} \cos(2 p_k(\lambda) \cdot z) \right] . \tag{23}$$

Since $\sin(-\theta) = \sin(\theta)$, and, since $\mathbb{V}_{n-1}$ is a symmetric set, it follows that $\sum_{z \in \mathbb{V}_{n-1}} \sin(2 p_k(\lambda) \cdot z) = 0$. Thus, since $e^{\mathrm{i}\theta} = \cos\theta + \mathrm{i} \sin\theta$,

$$2^{-(n-1)} \sum_{z \in \mathbb{V}_{n-1}} e^{\mathrm{i} 2 p_k(\lambda) \cdot z} = 2^{-(n-1)} \sum_{z \in \mathbb{V}_{n-1}} \cos(2 p_k(\lambda) \cdot z) . \tag{24}$$

Combining (23) and (24) shows that if ξ is a random uniformly distributed element of $\mathbb{V}_{n-1}$, then

$$|\psi(\lambda)|^2 \le \frac{1}{2}\left[1 + \mathbb{E}\left(e^{\mathrm{i}2p_k(\lambda)\cdot\xi}\right)\right]. \tag{25}$$

The coordinates $\xi_1, \ldots, \xi_{n-1}$ of ξ are independent unbiased random ± 1's. Therefore, because the components of $p_k(\lambda)$ are $\{\lambda_{\{i,k\}} : i \neq k\}$,

$$\begin{aligned} \mathbb{E}\left(e^{\mathrm{i}2p_k(\lambda)\cdot\xi}\right) &= \prod_{j=1}^{n-1} \mathbb{E}\left(e^{\mathrm{i}2[p_k(\lambda)]_j \xi_j}\right) \\ &= \prod_{i\,:\,i\neq k}\left[\frac{1}{2}e^{\mathrm{i}2\lambda_{\{i,k\}}} + \frac{1}{2}e^{-\mathrm{i}2\lambda_{\{i,k\}}}\right] = \prod_{i\,:\,i\neq k}\cos 2\lambda_{\{i,k\}}. \end{aligned} \tag{26}$$

Substituting (26) into (25) establishes (18).

Next we deal with the bounds for $\mathrm{Re}(\psi(\lambda))$ and $\mathrm{Im}(\psi(\lambda))$. We use the following bounds on the remainder in the Taylor expansion of the exponential: For $a \ge 0$ and b real,

$$\left| e^{-a} - \sum_{s=0}^{k} \frac{(-a)^s}{s!} \right| \le \min\left\{ \frac{2|a|^k}{k!}, \frac{|a|^{k+1}}{(k+1)!} \right\}, \tag{27}$$

$$\left| e^{\mathrm{i}b} - \sum_{s=0}^{k} \frac{(\mathrm{i}b)^s}{s!} \right| \le \min\left\{ \frac{2|b|^k}{k!}, \frac{|b|^{k+1}}{(k+1)!} \right\}. \tag{28}$$

(Equation (28) can be found as, for example, [1, equation 26.4]; the derivation of equation (27) is similar.) Equation (27) with $k = 2$ implies

$$\left| e^{-\frac{1}{2}\|\lambda\|^2} - (1 - \tfrac{1}{2}\|\lambda\|^2) \right| \le \tfrac{1}{6}\|\lambda\|^4; \tag{29}$$

equation (28) with $k = 2$ implies

$$\left| e^{\mathrm{i}\lambda\cdot Z(y)} - \left[1 + \mathrm{i}\lambda\cdot Z(y)\right] \right| \le \tfrac{1}{2}(\lambda\cdot Z(y))^2;$$

equation (28) with $k = 3$ implies

$$\begin{aligned} &\left| e^{\mathrm{i}\lambda\cdot Z(y)} - \left[1 + \mathrm{i}\lambda\cdot Z(y) - \tfrac{1}{2}(\lambda\cdot Z(y))^2 - \tfrac{\mathrm{i}}{6}(\lambda\cdot Z(y))^3\right] \right| \\ &\qquad\qquad\qquad\qquad \le \tfrac{1}{24}(\lambda\cdot Z(y))^4. \end{aligned}$$

Since $|\mathrm{Re}(z)| \le |z|$ and $|\mathrm{Im}(z)| \le |z|$ for all $z \in \mathbb{C}$, we have

$$\left|\mathrm{Im}(e^{\mathrm{i}\lambda\cdot Z(y)}) - \left[\lambda\cdot Z(y) - \tfrac{1}{6}(\lambda\cdot Z(y))^3\right]\right| \le \tfrac{1}{24}(\lambda\cdot Z(y))^4\,, \tag{30}$$

$$\left|\mathrm{Re}(e^{\mathrm{i}\lambda\cdot Z(y)}) - \left[1 - \tfrac{1}{2}(\lambda\cdot Z(y))^2\right]\right| \le \tfrac{1}{24}(\lambda\cdot Z(y))^4\,, \tag{31}$$

$$\left|\mathrm{Re}(e^{\mathrm{i}\lambda\cdot Z(y)}) - 1\right| \le \tfrac{1}{2}(\lambda\cdot Z(y))^2\,. \tag{32}$$

Let ξ be a uniform random element of $\mathbb{V}_n$. From (30),

$$\begin{aligned}\Big|\mathbb{E}\left[\mathrm{Im}(e^{\mathrm{i}\lambda\cdot Z(\xi)})\right] &- \mathbb{E}\left[\lambda\cdot Z(\xi) + \tfrac{1}{6}(\lambda\cdot Z(\xi))^3\right]\Big| \\ &\le \mathbb{E}\left|\mathrm{Im}(e^{\mathrm{i}\lambda\cdot Z(\xi)}) - \left[\lambda\cdot Z(\xi) + \tfrac{1}{6}(\lambda\cdot Z(\xi))^3\right]\right| \\ &\le \mathbb{E}\left[\tfrac{1}{24}(\lambda\cdot Z(\xi))^4\right] \end{aligned} \tag{33}$$

Since Im is linear, $\mathbb{E}\left[\mathrm{Im}(e^{\mathrm{i}\lambda\cdot Z(\xi)})\right] = \mathrm{Im}\,(\psi(\lambda))$, whence (33) implies

$$\left|\mathrm{Im}\,(\psi(\lambda)) - \mathbb{E}\,[\lambda\cdot Z(\xi)] - \tfrac{1}{6}\mathbb{E}\left[(\lambda\cdot Z(\xi))^3\right]\right| \le \mathbb{E}\left[\tfrac{1}{24}(\lambda\cdot Z(\xi))^4\right]\,. \tag{34}$$

Similarly, we have

$$\left|\mathrm{Re}(\psi(\lambda)) - \left(1 - \tfrac{1}{2}\mathbb{E}[(\lambda\cdot Z(\xi))^2]\right)\right| \le \tfrac{1}{24}\mathbb{E}[(\lambda\cdot Z(\xi))^4]\,, \tag{35}$$

and

$$\left|\mathrm{Re}(\psi(\lambda)) - 1\right| \le \tfrac{1}{2}\mathbb{E}[(\lambda\cdot Z(\xi))^2]\,. \tag{36}$$

Our goal now is to compute the above expectations. For all non-negative integers s,

$$\mathbb{E}[(\lambda\cdot Z(\xi))^s] = \sum_{1\le k_1<\ell_1\le n}\ \sum_{1\le k_2<\ell_2\le n} \cdots \sum_{1\le k_s<\ell_s\le n}\ \prod_{j=1}^{s} \lambda_{k_j\ell_j}\,\mathbb{E}\Big[\prod_{j=1}^{s}\xi_{k_j}\xi_{\ell_j}\Big]\,.$$

For each multi-set $S = \{\{k_1,\ell_1\},\{k_2,\ell_2\},\ldots,\{k_s,\ell_s\}\}$, let N_S be the network on the vertices $\{1,2,\ldots,n\}$ with the edge set S, where repeated elements in S correspond to multiple edges between vertices. Observe that

$$\mathbb{E}\left[\prod_{j=1}^{s}\xi_{k_j}\xi_{\ell_j}\right] = \begin{cases}1 & \text{if all vertices in } N_s \text{ have even degree,}\\ 0 & \text{otherwise}\,.\end{cases}$$

Therefore,

$$\mathbb{E}[(\lambda\cdot Z(\xi))^s] = \sum_{N_S} w(N_S) \prod_{\{k,\ell\}\in S} \lambda_{\{k,\ell\}}\,.$$

Here N_S ranges over all the networks on the vertices $\{1,2,\ldots,n\}$ having s edges and all degrees even, and $w(N_S)$ is a multinomial coefficient determined by the number of times each edge appears in N_S.

For $s = 1$, there are no even-degree networks. Therefore,

$$\mathbb{E}[\lambda \cdot Z(\xi)] = 0\,.$$

For $s = 2$, the even-degree networks are the two-vertex networks N_S with a single repeated edge $S = \{\{k_1, \ell_1\}, \{k_1, \ell_1\}\}$, and the weights $w(N_S)$ all equal $2!/2! = 1$. Thus

$$\mathbb{E}[(\lambda \cdot Z(\xi))^2] = \|\lambda\|^2\,.$$

Equation (36) therefore implies that

$$\Big|\mathrm{Re}(\psi(\lambda)) - 1\Big| \leq \tfrac{1}{2}\|\lambda\|^2\,,$$

from which (19) follows.

For $s = 3$, the even-degree networks are just triangles with the edges

$$\{\{k_1, k_2\}, \{k_2, k_3\}, \{k_1, k_3\}\}\,,$$

where $1 \leq k_1 < k_2 < k_3 \leq n$, and the weights $w(N_S)$ are all $3!/(1!)^3$, as there are three edges and each edge appears just once. Therefore,

$$\mathbb{E}\left[(\lambda \cdot Z(\xi))^3\right] = \sum_{i<j<k} 3!\lambda_{\{i,j\}}\lambda_{\{j,k\}}\lambda_{\{i,k\}}\,.$$

Thus the inequalities (34) and (35) become

$$\Big|\mathrm{Im}(\psi(\lambda)) + \sum_{i<j<k} \lambda_{\{i,j\}}\lambda_{\{j,k\}}\lambda_{\{i,k\}}\Big| \leq \tfrac{1}{24}\mathbb{E}[(\lambda \cdot Z(\xi))^4]\,, \tag{37}$$

$$\Big|\mathrm{Re}(\psi(\lambda)) - \big(1 - \tfrac{1}{2}\|\lambda\|^2\big)\Big| \leq \tfrac{1}{24}\mathbb{E}[(\lambda \cdot Z(\xi))^4]\,. \tag{38}$$

Moreover, applying the triangle inequality to the inequalities (29) and (38) shows that

$$\Big|\mathrm{Re}(\psi(\lambda)) - e^{-\frac{1}{2}\|\lambda\|^2}\Big| \leq \tfrac{1}{6}\|\lambda\|^4 + \tfrac{1}{24}\mathbb{E}[(\lambda \cdot Z(\xi))^4]\,. \tag{39}$$

Finally, for $s = 4$, there are several classes: (a) 4-cycles, (b) an edge repeated four times, (c) two non-adjacent edges repeated twice, and (d) two adjacent edges repeated twice. Thus

$$\begin{aligned}\mathbb{E}\left[(\lambda \cdot Z(\xi))^4\right] = \sum_{i_1<j_2} \lambda^4_{\{i_1,i_2\}} + 4!/(2!)^2 \sum_{\substack{\{i_1,i_2\}\\ \neq\{i_3,i_4\}}} \lambda^2_{\{i_1,i_2\}}\lambda^2_{\{i_3,i_4\}} \\ + 4! \sum_{\substack{i_1,i_2,i_3,i_4\\ \text{distinct}}} \lambda_{\{i_1,i_2\}}\lambda_{\{i_2,i_3\}}\lambda_{\{i_3,i_4\}}\lambda_{\{i_4,i_1\}}\,.\end{aligned}$$

Therefore, for $\lambda \in \mathrm{B}_\delta$,

$$\mathbb{E}\left[(\lambda \cdot Z(\xi))^4\right] \leq \tfrac{1}{2}n^2\delta^4 + \tfrac{3}{4}n^4\delta^4 + n^4\delta^4\,,$$

and, because we always assume $n \geq 3$,

$$\mathbb{E}\left[(\lambda \cdot Z(\xi))^4\right] \leq (\tfrac{1}{18} + \tfrac{3}{4} + 1)(n\delta)^4 \leq \tfrac{11}{6}(n\delta)^4 . \tag{40}$$

Consequently, the inequalities (37) and (38) imply

$$\begin{aligned} \Big| \mathrm{Im}(\psi(\lambda)) + \sum_{i<j<k} \lambda_{\{i,j\}}\lambda_{\{j,k\}}\lambda_{\{i,k\}} \Big| &\leq \tfrac{1}{12}(n\delta)^4 , \\ \Big| \mathrm{Re}(\psi(\lambda)) - \big(1 - \tfrac{1}{2}\|\lambda\|^2\big) \Big| &\leq \tfrac{1}{12}(n\delta)^4 . \end{aligned} \tag{41}$$

This last inequality gives us the estimate on $\mathrm{Im}(\psi(\lambda))$ claimed in (21).

We now use (41) to prove the estimate on $\mathrm{Re}(\psi(\lambda))$ stated in (20). Because $n \geq 3$, we have $\|\lambda\|^4 \leq (\frac{1}{2}n^2\delta^2)^2 \leq \frac{1}{36}(n\delta)^4$. Therefore, the equations (39) and (40) imply

$$\Big| \mathrm{Re}(\psi(\lambda)) - e^{-\frac{1}{2}\|\lambda\|^2} \Big| \leq \tfrac{1}{216}(n\delta)^4 + \tfrac{11}{144}(n\delta)^4 < \tfrac{1}{12}(n\delta)^4 .$$

Therefore, since $e^{-\frac{1}{2}\|\lambda\|^2} \geq e^{-\frac{1}{2}n^2\delta^2}$ for $\lambda \in \mathrm{B}_\delta$, it follows that

$$\Big| \frac{\mathrm{Re}(\psi(\lambda))}{e^{-\frac{1}{2}\|\lambda\|^2}} - 1 \Big| \leq \frac{\frac{1}{12}(n\delta)^4}{e^{-\frac{1}{2}\|\lambda\|^2}} < \frac{\frac{1}{12}(n\delta)^4}{e^{-\frac{1}{2}n^2\delta^2}} .$$

Therefore,

$$\mathrm{Re}(\psi(\lambda)) = e^{-\frac{1}{2}\|\lambda\|^2} \left[\frac{\mathrm{Re}(\psi(\lambda))}{e^{-\frac{1}{2}\|\lambda\|^2}} \right] = e^{-\frac{1}{2}\|\lambda\|^2} (1 + \varepsilon_1(\lambda)) ,$$

where

$$\big|\varepsilon_1(\lambda)\big| = \left| \frac{\mathrm{Re}(\psi(\lambda))}{e^{-\frac{1}{2}\|\lambda\|^2}} - 1 \right| \leq \tfrac{1}{12}(n\delta)^4 e^{\frac{1}{2}n^2\delta^2} .$$

■

We now bound the contribution of the secondary region to the integral $I(d,t)$.

Proposition 3.2.

$$\left| (2\pi)^{-d} \int_{R_\delta} \psi(\lambda)^t d\lambda \right| \leq e^{-\frac{11}{24}t\delta^2} .$$

Proof. By (18), for all $k \in \{1, 2, \ldots, n\}$,

$$|\psi(\lambda)|^2 \leq \tfrac{1}{2} + \tfrac{1}{2} \prod_{i\,:\,i \neq k} \cos(2\lambda_{\{i,k\}}) .$$

Let $\gamma \in R_\delta$. By Lemma 2.7, either there is an element $\lambda \in \Lambda_1 + \Lambda_2^{\mathrm{even}}$ such that $\gamma \in \mathrm{B}_{\pi/4}(\lambda) \setminus \mathrm{B}_\delta(\lambda)$, or there is an element $\lambda \in \Lambda_1 + \Lambda_2^{\mathrm{odd}}$ such that $\gamma \in \mathrm{B}_{\pi/4}(\lambda)$. In the first case, $\gamma = \lambda^{(1)} + \lambda^{(2)} + \mu$, where

$\mu \in \mathrm{B}_{\pi/4} \setminus \mathrm{B}_\delta$ and $\lambda^{(i)} \in \Lambda_i$ for $i = 1, 2$. Thus, there are $a, b \in \{0, 1\}$ such that

$$|\cos(2\gamma_{\{i,j\}})| = |\cos(2\pi a + \pi b + 2\mu_{\{i,j\}})| = |\cos(2\mu_{\{i,j\}})|\,.$$

Whence,

$$|\psi(\gamma)|^2 \le \tfrac{1}{2} + |\tfrac{1}{2}\min_{\{i,j\}}\big\{\cos(2\gamma_{\{i,j\}})\big\}| \le \tfrac{1}{2} + \tfrac{1}{2}\cos(2\delta) = \cos^2\delta\,.$$

In the second case, there is a choice of $k \in \{1, 2, \ldots, n\}$ such that an odd number of the components $\lambda_{\{i,k\}}$ $(i \ne k)$ are $\frac{\pi}{2}$. For this value of k, we have

$$\prod_{i \ne k} \cos(2\gamma_{\{i,k\}}) \le 0\,.$$

Therefore, in this case, we trivially have $|\psi(\gamma)|^2 \le (1/2) \le \cos^2\delta$, since $\delta \le \pi/4$. Therefore,

$$|\psi(\gamma)|^2 \le \cos^2\delta \qquad (\forall\ \gamma \in R_\delta).$$

Using the inequalities $\cos x \le 1 - x^2/2 + x^4/24$ and $1 - x \le e^{-x}$ yields

$$\cos\delta \le 1 - \frac{\delta^2}{2} + \frac{\delta^4}{24} \le e^{-\frac{\delta^2}{2}(1-\frac{\delta^2}{12})} \le e^{-\frac{11}{24}\delta^2}\,.$$

Therefore, for all $\gamma \in R_\delta$, we have $|\psi(\gamma)^t| < e^{-\frac{11}{24}t\delta^2}$, and hence we certainly have

$$(2\pi)^{-d}\left|\int_{R_\delta}\psi(\gamma)^t d\gamma\right| \le (2\pi)^{-d}\int_{R_\delta}|\psi(\gamma)^t| d\gamma < e^{-\frac{11}{24}t\delta^2}\,.$$

■

4. An Estimate for the Return Probabilities

We use our estimates obtained in the previous section for $\psi(\lambda)$ to obtain upper and lower bounds for the integral

$$P_n^{(t)}(0,0) = \frac{1}{(2\pi)^d}\int_{\mathrm{B}_\pi}\psi(\lambda)^t d\lambda\,. \tag{42}$$

Define

$$U(n,t,\delta) = \left[1 + \tfrac{1}{9}(n\delta)^6\right]^{t/2}\left[1 + \tfrac{1}{12}(n\delta)^4\right]^t\left[1 - e^{-t\delta^2}\right]^{d/2}, \tag{43}$$

$$L(n,t,\delta) = \left[1 + \tfrac{4}{9}t^2(n\delta)^6\right]^{-\frac{1}{2}}\left[1 - \tfrac{1}{12}(n\delta)^4\right]^t\left[1 - e^{-\frac{1}{2}t\delta^2}\right]^{d/2}. \tag{44}$$

$$U(n, 4t, \delta) = \left[1 + \tfrac{1}{9}(n\delta)^6\right]^{2t}\left[1 + \tfrac{1}{12}(n\delta)^4\right]^{4t}\left[1 - e^{-4t\delta^2}\right]^{d/2}, \tag{45}$$

$$L(n, 4t, \delta) = \left[1 + \tfrac{4}{9}(4t)^2(n\delta)^6\right]^{-\frac{1}{2}}\left[1 - \tfrac{1}{12}(n\delta)^4\right]^{4t}\left[1 - e^{-2t\delta^2}\right]^{d/2}. \tag{46}$$

Theorem 4.1. *Suppose that $n\delta \in (0, 1)$, and let t be a positive integer. Let $U(n, 4t, \delta)$ and $L(n, 4t, \delta)$ be as defined in (45) and (46), respectively. Then*

$$P_n^{(4t)}(0, 0) \leq 2^{2d-n+1}(8\pi t)^{-d/2}U(n, 4t, \delta) + e^{-\frac{11}{6}t\delta^2}. \tag{47}$$

Moreover, if $4t(n\delta)^3 < 1$, then

$$P_n^{(4t)}(0, 0) \geq 2^{2d-n+1}(8\pi t)^{-d/2}L(n, 4t, \delta) - e^{-\frac{11}{6}t\delta^2}. \tag{48}$$

Proof. Rearranging equation (6) we have

$$P_n^{(4t)}(0, 0) - 2^{2d-n+1}(2\pi)^{-d}\int_{\mathrm{B}_\delta}\psi(\gamma)^{4t}d\gamma = (2\pi)^{-d}\int_{R_\delta}\psi(\gamma)^t d\gamma\,;$$

By Proposition 3.2,

$$\left|P_n^{(4t)}(0, 0) - 2^{2d-n+1}(2\pi)^{-d}\int_{\mathrm{B}_\delta}\psi(\gamma)^{4t}d\gamma\right| \leq (2\pi)^d e^{-\frac{11}{6}t\delta^2}.$$

Thus, it is sufficient to prove that, for t satisfying the conditions of the theorem,

$$(8\pi t)^{-\frac{d}{2}}L(n, 4t, \delta) < (2\pi)^{-d}\int_{\mathrm{B}_\delta}\psi(\gamma)^{4t}d\gamma < (8\pi t)^{-\frac{d}{2}}U(n, 4t, \delta). \tag{49}$$

First note that, since $\psi(-\gamma)$ is the complex conjugate of $\psi(\gamma)$,

$$\int_{\mathrm{B}_\delta}\psi(\gamma)^{4t}d\gamma = \int_{\mathrm{B}_\delta}\mathrm{Re}\big(\psi(\gamma)^{4t}\big)d\gamma. \tag{50}$$

Therefore, we only need to understand the real part of the powers of ψ. In this proof, we employ Proposition A.2 to obtain upper and lower bounds on $\mathrm{Re}(z^k)$ in terms of $\mathrm{Re}(z)^k$. The bounds are sharpest when the ratio $\beta(z) := \mathrm{Im}(z)/\mathrm{Re}(z)$ has small magnitude. Lemma 3.1 implies that, for $\lambda \in \mathrm{B}_\delta$,

$$\begin{aligned}|\beta(\psi(\lambda))| &\leq \frac{\sum_{i<j<k}|\lambda_{\{i,j\}}\lambda_{\{j,k\}}\lambda_{\{k,i\}}| + \varepsilon_2(\lambda)}{1 - \frac{1}{2}\|\lambda\|^2} \\ &\leq \frac{\frac{1}{6}(n\delta)^3 + \frac{1}{12}(n\delta)^4}{1 - \frac{1}{4}(n\delta)^2} \leq \tfrac{1}{3}(n\delta)^3.\end{aligned}$$

The inequality (66) then implies that

$$\mathrm{Re}(\psi(\gamma)^{4t}) \leq \mathrm{Re}(\psi(\gamma))^{4t}\left[1 + \frac{(n\delta)^6}{9}\right]^{2t}. \tag{51}$$

Proposition A.2 also supplies a lower bound for $\mathrm{Re}(\psi(\gamma)^{4t})$. However, this bound only holds for powers $4t$ which satisfy the condition $\alpha(z) := 1 - \binom{4t}{2}\beta^2(z) > 0$.

We write β and α for $\beta(\psi(\gamma))$ and $\alpha(\psi(\gamma)) = 1 - \binom{4t}{2}\beta^2$, respectively. Suppose that $4t < 3(n\delta)^{-3}$. Then $4t\beta < 1$, and so $\alpha > 1/2$. In particular, $\alpha > 0$, whence (69) can be applied to obtain

$$\begin{aligned}\mathrm{Re}(\psi(\gamma)^{4t}) &\geq \mathrm{Re}(\psi(\gamma))^{4t}\Big[1+\beta^2\Big]^{2t}\Big[1+\Big(\frac{4t}{\alpha}\Big)^2\beta^2\Big]^{-1/2}\\ &\geq \mathrm{Re}(\psi(\gamma))^{4t}\Big[1+\Big(\frac{\beta}{\alpha}\Big)^2\beta^2\Big]^{-1/2}.\end{aligned}$$

Since $\alpha \geq 1/2$ and $\beta^2 \leq (n\delta)^3/3$, it follows that $\beta^2/\alpha^2 \leq (4/9)(n\delta)^6$ and thus

$$\mathrm{Re}(\psi(\gamma)^{4t}) \geq \mathrm{Re}(\psi(\gamma))^{4t}\left[1+\tfrac{4}{9}(4t)^2(n\delta)^6\right]^{-\frac{1}{2}}.$$

The above bound and (51) imply that

$$\begin{aligned}\left[1+\tfrac{4}{9}(4t)^2(n\delta)^6\right]^{-\frac{1}{2}}&\int_{\mathrm{B}_\delta}\mathrm{Re}\big(\psi(\gamma)\big)^{4t}d\gamma\\ &\leq \int_{\mathrm{B}_\delta}\mathrm{Re}\big(\psi(\gamma)^{4t}\big)d\gamma\\ &\leq \left[1+\tfrac{1}{9}(n\delta)^6\right]^{2t}\int_{\mathrm{B}_\delta}\mathrm{Re}\big(\psi(\gamma)\big)^{4t}d\gamma \qquad (52)\end{aligned}$$

We now turn to bounding $\int_{\mathrm{B}_\delta}\mathrm{Re}(\psi(\gamma))^{4t}d\gamma$. Equation (20) of Lemma 3.1 implies that

$$\psi(\gamma) = e^{\frac{1}{2}\|\gamma\|^2}\left[1+\varepsilon_1(\gamma)\right],$$

where $|\varepsilon_1(\gamma)| < \frac{1}{12}(n\delta)^4$. Notice that this estimate is ideal when we need an estimate for powers of $\psi(\gamma)$. Moreover, the real part of $1+\varepsilon_1(\gamma)$ must lie between $1+\frac{1}{12}(n\delta)^4$ and $1-\frac{1}{12}(n\delta)^4$. Therefore, we have

$$\left[1+\tfrac{1}{12}(n\delta)^4\right]^{4t}e^{-\frac{4t}{2}\|\gamma\|^2} \geq \mathrm{Re}(\psi(\lambda))^{4t} \geq \left[1-\tfrac{1}{12}(n\delta)^4\right]^{4t}e^{-\frac{4t}{2}\|\gamma\|^2}. \quad (53)$$

If we let

$$J(d,t,\delta) := \int_{\mathrm{B}_\delta} e^{-\frac{t}{2}\sum_{j<k}\gamma^2_{\{j,k\}}}\,d\gamma\,,$$

then (52) and (53) imply that

$$\begin{aligned}\Big[1+\tfrac{4}{9}(4t)^2(n\delta)^6\Big]^{-1/2}&\left[1-\tfrac{1}{12}(n\delta)^4\right]^{4t}J(d,4t,\delta)\\ &\leq \int_{\mathrm{B}_\delta}\mathrm{Re}(\psi(\gamma))^{4t}d\gamma\\ &\leq \left[1+\tfrac{1}{9}(n\delta)^6\right]^{2t}\left[1+\tfrac{1}{12}(n\delta)^4\right]^{4t}J(d,4t,\delta)\,. \qquad (54)\end{aligned}$$

To complete the proof, it remains to obtain suitable bounds for the integral $J(d,n,t)$. Changing variables by letting $\mu_{\{j,k\}} = \gamma_{\{j,k\}}\sqrt{t}$ yields

$$J(d,t,\delta) = t^{-d/2} \int_{\mathrm{B}_{\delta\sqrt{t}}} e^{-\frac{1}{2}\sum_{j<k}\mu^2_{\{j,k\}}}\, d\mu\,.$$

Now, for all $\rho > 0$, we have

$$\int_0^{\rho^2} 2\pi r e^{-\frac{1}{2}r^2}\, dr < \int_{[-\rho,\,\rho]^2} e^{-\frac{1}{2}(\alpha^2+\beta^2)}\, d\alpha\, d\beta < \int_0^{2\rho^2} 2\pi r e^{-\frac{1}{2}r^2}\, dr\,.$$

So

$$\sqrt{2\pi\,(1-e^{-\rho^2/2})} < \int_{[-\rho,\,\rho]} e^{-\mu^2_{\{j,k\}}/2} d\mu_{\{j,k\}} < \sqrt{2\pi\,(1-e^{-\rho^2})}\,.$$

Therefore

$$\left(\frac{2\pi}{t}\right)^{d/2}\left(1-e^{-t\delta^2/2}\right)^{d/2} \;<\; J(d,t,\delta) \;<\; \left(\frac{2\pi}{t}\right)^{d/2}\left(1-e^{-t\delta^2}\right)^{d/2}.$$

Combining this with (54), and using (50), establishes (49), completing the proof. ■

We can now derive the asymptotic formula for $N_{n,4t}$ in Theorem 2.

Proof of Theorem 2. Fix n and let $\delta = t^{-5/12}$. Then $4t(n\delta)^3 = 4n^3t^{-1/4}$, which for large enough t is less than 1, so the bound (48) can be used. Note that $t^2\delta^6 = t^{-1/2}$, whence $[1+(4/9)(4t)^2(n\delta)^6]^{-1/2} \to 1$ as $t\to\infty$. Also, for any constant c_n,

$$\left(1-c_n t^{-5/3}\right)^t = e^{-c_n t^{-2/3}}[1+o(1)] \to 1 \quad \text{as } t\to\infty\,,$$

whence $[1-(1/12)(n\delta)^4]^{4t} \to 1$ as $t\to\infty$. Finally, $t\delta^2 = t^{1/6}$, so $[1-e^{-2t\delta^2}]^{d/2} \to 1$ as $t\to\infty$. We conclude that $L(n,4t,t^{-5/12}) \to 1$. This together with (48) implies that

$$\liminf_{t\to\infty} \frac{P_n^{4t}(0,0)}{2^{2d-n+1}(8\pi t)^{-d/2}} \ge \lim_{t\to\infty}\left[L(n,4t,t^{-5/12}) - \frac{e^{-\frac{11}{6}t^{1/6}}}{2^{2d-n+1}(8\pi t)^{-d/2}}\right] = 1\,. \quad (55)$$

Similarly, $U(n,4t,t^{-5/12}) \to 1$, which with (47) implies that

$$\limsup_{t\to\infty} \frac{P_n^{4t}(0,0)}{2^{2d-n+1}(8\pi t)^{-d/2}} \le \lim_{t\to\infty}\left[U(n,4t,t^{-5/12}) - \frac{e^{-\frac{11}{6}t^{1/6}}}{2^{2d-n+1}(8\pi t)^{-d/2}}\right] = 1\,. \quad (56)$$

The inequalities (55) and (56), with the identity $N_{n,4t} = 2^{nt}P_n^{4t}(0,0)$, prove (2). ■

5. Implications for the Existence and Abundance of Partial Hadamard Matrices

In this section, we show how our upper and lower bounds for the integral $I(d,t)$ imply statements about the existence and abundance of partial Hadamard matrices. We will answer the following questions:

- When does the upper bound (47) imply a non-trivial bound on the number $N_{n,t}$ of partial Hadamard matrices?
- When does the lower bound (48) exceed zero, and hence imply that there is an $n \times t$ partial Hadamard matrix?

Let $N_{n,t}$ denote the number of $n \times t$ partial Hadamard matrices, and let

$$\begin{aligned} A(n,t) &:= 2^{2d-n+1}(2\pi t)^{-d/2}\,, \\ R(n,t) &:= N_{n,t}/2^{nt}A(n,t)\,. \end{aligned}$$

Recalling the definitions in (45) and (46), let $U(n,t)$ and $L(n,t)$ be defined as

$$\begin{aligned} U(n,t) &:= \min_{\delta<n^{-1}} \left\{ U(n,t,\delta) + A(n,t)^{-1}e^{-\frac{11}{24}t\delta^2} \right\}, \\ L(n,t) &:= \max_{\delta<n^{-1}} \left\{ L(n,t,\delta) - A(n,t)^{-1}e^{-\frac{11}{24}t\delta^2} \right\}. \end{aligned}$$

By Theorem 4.1,

$$L(n,4t) \ \le \ R(n,4t) \ \le \ U(n,4t)\,.$$

Theorem 5.1.

(i) **Abundance of Designs**. *For all sufficiently large n, and $t > n^8$,*

$$R(n,t) \le e^{n^4 t^{-\frac{1}{2}}} + t^{\frac{d}{2}} e^{-\frac{11}{24}t^{\frac{1}{4}}}\,.$$

(ii) **Existence of Designs**. *For all $\alpha, \beta > 0$, and n sufficiently large, we have*

$$L(n, t = n^{12+3\beta+2\alpha}) > e^{-\frac{1}{4}n^{-2\alpha}} + A(n,t)^{-1}e^{-\frac{11}{24}n^{2+\beta}}\,.$$

For all sufficiently large n, there is an $n \times 4t$ partial Hadamard matrix for all $t > n^{12}$.

Proof. We bound the function $U(n,t)$ by obtaining separate bounds for the logarithms of the two pieces:

$$u_1(n,t,\delta) := A(n,t)^{-1}e^{-\frac{11}{24}t\delta^2} \quad \text{and} \quad U(n,t,\delta)\,.$$

For $U(n,t)$ to be small, the logarithm

$$\log\left[u_1(n,t,\delta)\right] = -\tfrac{11}{24}t\delta^2 - (2d-n+1)\log 2 + \tfrac{d}{2}\log(2\pi) + \tfrac{d}{2}\log t$$

of the first piece must be negative and large in absolute value. Therefore, for fixed n, as t grows the quantity $t\delta^2$ must grow. So we put $\delta = t^{-\frac{1}{2}+\varepsilon}$, where $\varepsilon > 0$ is small. Since we require $\delta < n^{-1}$, we must be sure that $t^{\frac{1}{2}-\varepsilon} > n$. In any case, setting $\delta = t^{-\frac{1}{2}+\varepsilon}$, the expression for $\log(u_1(n,t,\delta))$ becomes

$$f_\varepsilon(t) = -\tfrac{11}{24}t^{2\varepsilon} + \tfrac{d}{2}\log t - (2d-n+1)\log 2 + \tfrac{d}{2}\log(2\pi)\,.$$

Notice that

$$-(2d-n+1)\log 2 + \tfrac{d}{2}\log(2\pi) < 0\,.$$

Therefore

$$f_\varepsilon(t) \le -\tfrac{11}{24}t^{2\varepsilon} + \tfrac{d}{2}\log t := g_\varepsilon(t)\,. \tag{57}$$

For $\varepsilon > 0$, the function $g_\varepsilon(t)$ attains its maximum

$$m(\varepsilon) = \tfrac{1}{4}d\varepsilon^{-1}\left[\log\left(\tfrac{6}{11}d\varepsilon^{-1}\right) - 1\right]$$

at the point $t_0(\varepsilon) = \left(\frac{6}{11}d\varepsilon^{-1}\right)^{1/2\varepsilon}$. In particular, $t_0(1/8) = (\frac{48}{11}d)^4$ and $m(1/8) = 2d\log\left(\frac{48}{11}de^{-1}\right)$. Note that $g_{1/8}(n^9)$ is approximately $-n^{9/4}$, so, once t exceeds n^8, the function $f_\varepsilon(t)$ rapidly approaches zero. In any case, putting $\varepsilon = 1/8$ in (57), yields the bound

$$u_1(n,t,t^{-\frac{3}{8}}) \le t^{\frac{d}{2}}e^{-\frac{11}{24}t^{\frac{1}{4}}}\,. \tag{58}$$

We now examine the behavior of the second piece

$$U(n,t,\delta) = \left[1 + \tfrac{1}{9}(n\delta)^6\right]^{t/2}\left[1 + \tfrac{1}{12}(n\delta)^4\right]^{t}\left[1 - e^{-t\delta^2}\right]^{d/2}.$$

Since $1 + x \le e^x$, we have

$$\log U(n,t,\delta) \le \tfrac{1}{18}(n\delta)^6 t + \tfrac{1}{12}(n\delta)^4 t - \tfrac{1}{2}de^{-t\delta^2}\,.$$

Therefore,

$$\log U(n,t,t^{-1/2+\varepsilon}) \le \tfrac{1}{18}n^6t^{-2+6\varepsilon} + \tfrac{1}{12}n^4t^{-1+4\varepsilon} - \tfrac{1}{2}de^{-t^{2\varepsilon}}\,.$$

For $\varepsilon < 1/2$, and n fixed, the middle term eventually dominates as t grows. For $\varepsilon < 1/4$, this term approaches zero. Indeed, for $\varepsilon = 1/8$ and $t > n^8$, we have for n sufficiently large

$$U(n,t,t^{-\frac{3}{8}}) \le e^{n^4t^{-\frac{1}{2}}}\,.$$

Combining this with (58), for $t > n^8$ and n sufficiently large, we have

$$\begin{aligned} U(n,t) &:= \min_{\delta < n^{-1}}\{u_1(n,t,\delta) + U(n,t,\delta)\} \\ &\le u_1(n,t,t^{-\frac{3}{8}}) + U(n,t,t^{-\frac{3}{8}}) \le e^{n^4t^{-\frac{1}{2}}} + t^{\frac{d}{2}}e^{-\frac{11}{24}t^{\frac{1}{4}}}\,. \end{aligned}$$

This completes the proof of (i).

We now prove (ii). Recall from (46) that

$$L(n,t,\delta) = \left[1 + \tfrac{4}{9}t^2(n\delta)^6\right]^{-\frac{1}{2}}\left[1 - \tfrac{1}{12}(n\delta)^4\right]^t\left[1 - e^{-\frac{1}{2}t\delta^2}\right]^{d/2}.$$

For fixed n and t, we determine when there exists $\delta \in [0, n^{-1}]$ such that

$$\log L(n,t,\delta) > -\log A(n,t) - \tfrac{11}{24}t\delta^2\,, \tag{59}$$

ensuring that $L(n,t) > 0$. Since $e^{-2x} \leq 1 - x$ for $0 \leq x \leq 1/2$, and, since $e^x > 1 + x$,

$$\log L(n,t,\delta) \geq -\tfrac{2}{9}t^2(n\delta)^6 - \tfrac{1}{12}(n\delta)^4 t - \tfrac{1}{4}de^{-\frac{1}{2}t\delta^2}.$$

Thus (59) is satisfied if the right-hand side above exceeds the right-hand side of (59). After rearranging, this is equivalent to

$$\begin{aligned} &t\big(\tfrac{11}{24}\delta^2 - \tfrac{1}{12}(n\delta)^4 - \tfrac{2}{9}(n\delta)^6 t\big) \\ &\qquad \geq \tfrac{1}{2}d\log t + \tfrac{1}{2}d\big(\log(2\pi) + \tfrac{1}{2}e^{-\frac{1}{2}t\delta^2}\big) - (2d - n + 1)\log(2)\,. \end{aligned}$$

This inequality certainly holds if we drop the last two terms which contribute a comparatively small negative quantity as t grows. Thus we are led to consider the simpler inequality

$$t(\tfrac{11}{24}\delta^2 - \tfrac{1}{12}(n\delta)^4 - \tfrac{2}{9}(n\delta)^6 t) \geq \tfrac{1}{4}n^2\log t\,. \tag{60}$$

This inequality presents three challenges which we need to overcome. Firstly, we must ensure that the left-hand side is positive; so we must have

$$\tfrac{11}{24}\delta^2 \geq \tfrac{1}{12}(n\delta)^4 + \tfrac{2}{9}(n\delta)^6 t\,. \tag{61}$$

Secondly, we must find the smallest t for a given n for which the inequality has a feasible region for δ. Thirdly, we must ensure that the conditions

$$\delta < n^{-1} \qquad \text{and} \qquad t(n\delta)^3 < 1\,, \tag{62}$$

imposed by Theorem 4.1 hold.

Before we begin, it is helpful to consider the following simplified version of (60):

$$f_{a,b,c}(t) = \frac{t(a - bt)}{\log t} \geq cn^2\,,$$

where $a, b, c > 0$. For large t, the function $f_{a,b,c}(t)$ is essentially quadratic in t. So ignoring the effect of the $\log t$ term, we should expect there to be a solution if cn^2 is less than the maximum $\frac{1}{4}a^2b^{-1}$ attained by the function $f_{a,b,c}$. Moreover, the solution if it exists will lie in the interval $(0, a/b)$. The corresponding maximum and interval for

the inequality (60) are (dropping the constant coefficients which are immaterial to this argument)

$$(\delta^2(n\delta)^{-3} - (n\delta))^2 \qquad \text{and} \qquad \Big(0, (n\delta)^{-2}(n^{-4}\delta^{-2} - 1)\Big)\,.$$

Here we took $a = \delta^2 - (n\delta)^4$ and $b = (n\delta)^6$. So, if there is a solution, we must have

$$n < \delta^2(n\delta)^{-3} - (n\delta) < \delta^2(n\delta)^{-3}\,.$$

So, for n large, we must have $\delta^{-1} > n^4$. Putting $\delta = n^{-4-\varepsilon}$, where $\varepsilon > 0$, in (60) yields the simplified inequality

$$\frac{t}{\log t} \geq n^{10+2\varepsilon}\big(\tfrac{11}{6} - \tfrac{1}{3}n^{-4-2\varepsilon} - \tfrac{8}{9}n^{-10-4\varepsilon}t\big)^{-1}\,, \tag{63}$$

where the roles of the various terms on the left-hand side of the original inequality (60) are now clear. In particular, we now see that for any $\varepsilon > 0$, as n grows, there is a feasible region for δ when $t = n^{10+2\varepsilon+\beta}$, where $\beta > 0$, that the term $\frac{11}{24}t\delta^2$ is the important term, and that the term $\frac{2}{9}(n\delta)^6 t$ presents no difficulty: i.e., the condition (61) can be satisfied, provided that $\beta < 2\varepsilon$. Indeed, since $\delta = n^{-4-\varepsilon}$, the first part of condition (62) is already satisfied. However, the second part of (62) requires that $t(n\delta)^3 < 1$, which holds if and only if $4n^{1-\varepsilon+\beta} < 3$. Thus all conditions are satisfied for sufficiently large n provided that $\beta > 0$ and $\varepsilon > 1 + \beta$. Therefore, putting $\varepsilon = 1 + \alpha + \beta$, we have

$$t = n^{12+3\beta+2\alpha} \qquad \delta = n^{-5-\beta-\alpha} \qquad (\alpha, \beta > 0)$$

and, for all sufficiently large n, these values for t and δ satisfy all conditions. Feeding these parameters into the lower bound (59) for $\log\big(L(n,t,\delta)\big)$ yields the expression:

$$-\tfrac{1}{12}(4n^{-4-\beta-2\alpha}) - \tfrac{2}{9}n^{-2\alpha} - \tfrac{1}{4}de^{-\frac{1}{2}n^{2+\beta}}\,.$$

The middle term dominates for large n; so for sufficiently large n,

$$L(n, t = n^{12+3\beta+2\alpha}, \delta = n^{-5-\beta-\alpha}) > e^{-\frac{1}{4}n^{-2\alpha}}\,,$$

say, and, indeed,

$$L(n, t = n^{12+3\beta+2\alpha}) > e^{-\frac{1}{4}n^{-2\alpha}} + A(n,t)^{-1}e^{-\frac{11}{24}n^{2+\beta}}\,.$$

This completes the proof of (ii). ∎

6. The Branching Bound

In this section, we take advantage of the fact that the walk for partial Hadamard matrices with n rows contains, as projections, the walks for the partial Hadamard matrices with fewer rows than n. We exploit this structure to obtain an upper bound on the number of distinct $n \times 4t$ partial Hadamard matrices. We call this the *Branching Bound*.

The idea is that we can build up any $n \times t$ partial Hadamard matrix by the searching a tree $\mathcal{T}$, say whose nodes at level m correspond to the $m \times t$ partial Hadamard matrices. The parent of the node at level m corresponding to the matrix A is the node at level $m-1$ corresponding to the partial Hadamard matrix obtained by removing the last row of A. If we choose a total order on $\mathbb{V}_t$, then we can fully specify such a tree. Any total order on $\mathbb{V}_t$ imposes a total order on the set of $m \times t$ partial Hadamard matrices: matrix A is greater than matrix B if their first j rows agree, and the $(j+1)$-th row of matrix A is greater than the $(j+1)$-th row of B. Then we may suppose the i-th node at level m of $\mathcal{T}$ corresponds to the i-th $m \times t$ partial Hadamard matrix.

The following lemma allows us to bound the number of nodes at level $m+1$ in terms of the number of nodes at level m.

Lemma 6.1. *If $t \geq m$, then any m-dimensional real subspace of $\mathbb{R}^t$ contains at most 2^m elements of $\mathbb{V}_t$. Moreover, this bound can be attained for all $t \geq m$.*

Proof. Let $c^{(1)}, \ldots, c^{(\ell)} \in \mathbb{V}_t$ be ℓ vectors lying in some m-dimensional real subspace. Form the $t \times \ell$ matrix C whose i-th column is $c^{(i)}$:

$$C = \begin{bmatrix} c^{(1)} & c^{(2)} & \ldots & c^{(\ell)} \end{bmatrix} .$$

If needs be, we can re-order the columns of C so that the first m columns of C are linearly independent. (If not, then there is no set of m linearly independent columns, and the vectors all lie in an $m-1$ dimensional subspace.) Moreover, since the $t \times m$ matrix comprised of the first m columns of C has rank m, we may re-order the rows of C so that the $m \times m$ matrix B in the upper-left corner of C is invertible.

Now let $s > m$, and let $b^{(s)}$ be the m-dimensional vector comprised of the first m components of $c^{(s)}$. Since $c^{(s)}$ is a linear combination of the vectors $c^{(1)}, \ldots, c^{(m)}$, and since B is invertible, there is a unique m-dimension real vector $a^{(s)}$ such that $b^{(s)} = Ba^{(s)}$. Indeed, $c^{(s)} = Ca^{(s)}$. Notice that if $c^{(u)}$ is a different column of C such that $b^{(u)} = b^{(s)}$, then $c^{(u)} = c^{(s)}$. Therefore, since there are at most 2^m choices for $b^{(s)}$, we see that $\ell \leq 2^m$. ∎

We can now prove the following theorem:

Theorem 6.2. *$P_n^{(4t)}(0,0) \le 2^{n-1-4t} P_{n-1}^{(4t)}(0,0)$.*

Proof. For $z \in \mathbb{V}_{n-1}$, define

$$Q(z) = (z_j z_k)_{1 \le j < k \le n} \,.$$

The quantity $\mathbb{1}\{P\}$ equals 1 if property P holds, and zero otherwise. The number of $n \times t$ partial Hadamard matrices is exactly

$$\sum_{y^{(1)} \in \mathbb{V}_n} \cdots \sum_{y^{(t)} \in \mathbb{V}_n} \mathbb{1}\Big\{ \sum_{s=1}^{t} y_i^{(s)} y_j^{(s)} = 0 \quad \forall\, 1 \le i < j \le n \Big\} .$$

Letting $a_s = y_1^{(s)}$ for $s = 1, \dots, t$, this equals

$$\sum_{\substack{a_1 \in \{-1,1\} \\ (y_2^{(1)}, \dots, y_n^{(1)}) \in \mathbb{V}_{n-1}}} \cdots \sum_{\substack{a_t \in \{-1,1\} \\ (y_2^{(t)}, \dots, y_n^{(t)}) \in \mathbb{V}_{n-1}}} \mathbb{1}\left\{ \begin{array}{l} \sum_{s=1}^t y_i^{(s)} y_j^{(s)} = 0 \\ \forall\, 2 \le i < j \le n \end{array} \right\}$$
$$\times\, \mathbb{1}\left\{ \begin{array}{l} \sum_{s=1}^t a_s y_j^{(s)} = 0 \\ \forall\, 2 \le j \le n \end{array} \right\},$$

and the letting $z^{(s)} = (y_2^{(s)}, \dots, y_n^{(s)}) \in \mathbb{V}_{n-1}$, we obtain

$$\begin{aligned} & P_n^{(t)}(0,0) \\ & = 2^{-tn} \sum_{z^{(1)}, \cdots, z^{(t)} \in \mathbb{V}_{n-1}} \mathbb{1}\Big\{ \sum_{j=1}^{t} Q(z^{(j)}) = 0 \Big\} \sum_{a \in \mathbb{V}_t} \mathbb{1}\Big\{ \sum_{j=1}^{t} a_j z^{(j)} = 0 \Big\} . \end{aligned} \tag{64}$$

Next, we apply Lemma 6.1. If $\{z^{(1)}, \dots, z^{(t)}\}$ is a set of t elements of $\mathbb{V}_{n-1}$ satisfying $\sum_{j=1}^t Q(z^{(j)}) = 0$, then the $(n-1) \times t$ matrix $Z_t = [z^{(1)}, \dots, z^{(t)}]$ has rank $n-1$. So the solutions to $Z_t a = 0$ thus are contained in a $t-(n-1)$ vector subspace of $\mathbb{R}^t$. Then, by Lemma 6.1, the set of $a \in \mathbb{V}_t$ satisfying $\sum_{j=1}^t a_j z^{(j)} = 0$ has cardinality at most 2^{t-n+1}.

Thus,

$$\begin{aligned} P_n^{(t)}(0,0) &\le 2^{-n+1} \cdot 2^{-t(n-1)} \sum_{z^{(1)}, \cdots, z^{(t)} \in \mathbb{V}_{n-1}} \mathbb{1}\Big\{ \sum_{j=1}^{t} Q(z^{(j)}) = 0 \Big\} \\ &= 2^{-(n-1)}\, P_{n-1}^{(t)}(0,0) \,. \end{aligned}$$

■

The following corollary is immediate:

Corollary 6.3. *For $4t \geq n \geq s \geq 1$,*

$$P_n^{(4t)}(0,0) \leq 2^{-\binom{n}{2}+\binom{s}{2}}\, P_s^{(4t)}(0,0)\,.$$

In particular there are at most $2^{\binom{n+1}{2}}$ Hadamard matrices of order n.

This bound is clearly inexact. Direct arguments prove that

$$P_2^{(4t)}(0,0) = 2^{-4t}\binom{4t}{2}, \qquad \text{and} \qquad P_3^{(4t)}(0,0) = 2^{-8t}(4t)!/(t!)^4\,.$$

By using Stirling's Formula (with error bounds) to approximate the binomial coefficients above, one can see that the asymptotic formula in Theorem 2 is actually very good.

7. Conclusion

We have introduced a random walk for each integer $n \geq 3$ in which the probability of returning to the start of the walk after t steps is proportional to the number of distinct $n \times t$ partial Hadamard matrices. The behavior of this walk when t is close to n is of particular interest. This paper contains a preliminary analysis of this walk using Fourier theory on the d-dimensional integer lattice (here $d = \binom{n}{2}$) which shows how the walk behaves for t polynomial in n. Consequently, we are able to estimate the number of distinct $n \times t$ partial Hadamard matrices for $t > n^{12}$. Even this preliminary analysis yields new facts about designs.

This paper has also completed an important first step in the standard Fourier-theoretic approach to walks in a discrete lattice. We have been able to give a fairly complete description of the set of points $\lambda \in \mathrm{B}_\pi$, where the characteristic function $\psi(\lambda)$ has magnitude equal to one. In our case, the set has interesting combinatorial structure: for example, each point in the set corresponds to a graph on n vertices all of whose degrees are even. We have also obtained some estimates for the characteristic function by methods which give us a glimpse of the underlying combinatorial questions which will need to be studied in order to obtain better more global estimates for the characteristic function.

Finally, we note that the walks discussed in this paper are just one example of a walk corresponding to a familiar kind of combinatorial design. For example, we have carried out elsewhere most of the steps in this paper for the walks corresponding to balanced incomplete block designs.

Appendix A. Some Inequalities

In this appendix, we record and prove inequalities which relate $\mathrm{Re}(z)^t$ and $\mathrm{Re}(z^t)$.

We employ the following version of the Neyman-Pearson Lemma:

Lemma A.1. *Let $\lambda_0, \lambda_1, \ldots, \lambda_n$ be positive real numbers, and let*

$$A_0, A_1, \ldots, A_n \qquad \text{and} \qquad B_0, B_1, \ldots, B_n$$

be non-negative real numbers. Then

$$\min_{0\le s\le n}\left\{\frac{B_s}{A_s}\right\} \le \frac{\sum_{s=0}^n \lambda_s B_s}{\sum_{s=0}^n \lambda_s A_s} \le \max_{0\le s\le n}\left\{\frac{B_s}{A_s}\right\}.$$

Proof. Let s_0 and s_1 satisfy

$$\frac{B_{s_0}}{A_{s_0}} = \min_{0\le s\le n}\left\{\frac{B_s}{A_s}\right\} \qquad \text{and} \qquad \frac{B_{s_1}}{A_{s_1}} = \max_{0\le s\le n}\left\{\frac{B_s}{A_s}\right\}.$$

Then

$$\begin{aligned}\frac{B_{s_0}}{A_{s_0}} = \frac{\sum_{0\le s\le n}\lambda_s A_s (B_{s_0}/A_{s_0})}{\sum_{0\le s\le n}\lambda_s A_s} &\le \frac{\sum_{0\le s\le n}\lambda_s B_s}{\sum_{0\le s\le n}\lambda_s A_s}\\ &\le \frac{\sum_{0\le s\le n}\lambda_s A_s (B_{s_1}/A_{s_1})}{\sum_{0\le s\le n}\lambda_s A_s} = \frac{B_{s_1}}{A_{s_1}}.\end{aligned}$$

■

We can now prove the required inequalities relating $\mathrm{Re}(z^t)$ to $\mathrm{Re}(z)^t$.

Proposition A.2. *Let $t > 0$ be an integer.*

(i) *For any complex number we have*

$$\left\{\mathrm{Re}(z^{4t})\left(1+\left[\frac{\mathrm{Im}(z^{4t})}{\mathrm{Re}(z^{4t})}\right]^2\right)^{\frac{1}{2}}\right\}^2 = \left\{\left(1+\left[\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\right]^2\right)^{2t}\mathrm{Re}(z)^{4t}\right\}^2. \tag{65}$$

In particular,

$$\mathrm{Re}(z^{4t}) \le \mathrm{Re}(z)^{4t}\left(1+\left[\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\right]^2\right)^{2t}. \tag{66}$$

(ii) *If $\alpha = 1 - \binom{4t}{2}\left\{\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\right\}^2 > 0$, then*

$$\mathrm{Re}(z^{4t}) = \mathrm{Re}(z)^{4t}\left(1+\left[\frac{\mathrm{Im}(z^{4t})}{\mathrm{Re}(z^{4t})}\right]^2\right)^{-\frac{1}{2}}\left(1+\left[\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\right]^2\right)^{2t}. \tag{67}$$

(iii) *If $\alpha = 1 - \binom{4t}{2}\left\{\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\right\}^2 > 0$, then*

$$\left[\frac{\mathrm{Im}(z^{4t})}{\mathrm{Re}(z^{4t})}\right]^2 \le \left[\frac{4t}{\alpha}\right]^2\left[\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\right]^2. \tag{68}$$

(iv) *If* $\alpha = 1 - \binom{4t}{2}\left\{\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\right\}^2 > 0$, *then*

$$\mathrm{Re}(z^{4t}) \geq \mathrm{Re}(z)^{4t}\Big(1 + \Big[\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\Big]^2\Big)^{2t}\Big(1 + \Big[\frac{4t}{\alpha}\Big]^2\Big[\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\Big]^2\Big)^{-\frac{1}{2}}. \tag{69}$$

Proof. For any complex number z and any natural number t, we have

$$\Big[\mathrm{Re}(z^{4t})\Big\{1 + \Big(\frac{\mathrm{Im}(z^{4t})}{\mathrm{Re}(z^{4t})}\Big)^2\Big\}^{\frac{1}{2}}\Big]^2 = \mathrm{Re}(z^{4t})^2\Big\{1 + \Big(\frac{\mathrm{Im}(z^{4t})}{\mathrm{Re}(z^{4t})}\Big)^2\Big\} = |z^{4t}|^2\,,$$

and

$$(|z|^2)^{4t} = \Big[\Big\{1 + \Big(\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\Big)^2\Big\}\mathrm{Re}(z)^2\Big]^{4t} = \Big[\Big\{1 + \Big(\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\Big)^2\Big\}^{2t}\mathrm{Re}(z)^{4t}\Big]^2.$$

So equation (65) holds. This proves part (i).

To prove part (ii), we must show that if $\alpha > 0$, then $\mathrm{Re}(z^{4t})$ is non-negative. Suppose $z = a + \mathrm{i}b$ where a and b are real. Then

$$\mathrm{Re}(z^{4t}) = b^{4t} + a^{4t}\sum_{s=0}^{t-1}\binom{4t}{4s}\Big(\frac{b}{a}\Big)^{4s}\Big[1 - \frac{(4t-4s)(4t-4s-1)}{(4s+1)(4s+2)}\Big(\frac{b}{a}\Big)^2\Big],$$

and

$$\mathrm{Im}(z^{4t}) = a^{4t}\sum_{s=0}^{t-1}\Big\{\binom{4t}{4s+1}\Big(\frac{b}{a}\Big)^{4s+1} \times \Big[1 - \frac{(4t-4s-1)(4t-4s-2)}{(4s+2)(4s+3)}\Big(\frac{b}{a}\Big)^2\Big]\Big\}.$$

Since, for $s \in \{0, 1, \dots, t-1\}$,

$$\Big[1 - \frac{(4t-4s)(4t-4s-1)}{(4s+1)(4s+2)}\Big(\frac{b}{a}\Big)^2\Big] \geq 1 - \binom{4t}{2}\Big\{\frac{b}{a}\Big\}^2 = \alpha > 0\,,$$

we have $\mathrm{Re}(z^{4t}) > 0$. This proves part (ii).

We prove part (iii). If we put

$$\lambda_0 = 1, \quad \lambda_s = \binom{4t}{4s}\Big(\frac{b}{a}\Big)^{4s},$$

$$A_0 = b^{4t}\,, \quad A_s = \Big[1 - \frac{(4t-4s)(4t-4s-1)}{(4s+1)(4s+2)}\Big(\frac{b}{a}\Big)^2\Big],$$

and

$$B_0 = 0\,, \quad B_s = \Big(\frac{4t-4s}{4s+1}\Big)\Big[1 - \frac{(4t-4s-1)(4t-4s-2)}{(4s+2)(4s+3)}\Big(\frac{b}{a}\Big)^2\Big],$$

then

$$\mathrm{Re}(z^{4t}) = \sum_{s=0}^{t-1} \lambda_s A_s\,, \qquad \text{and} \qquad \mathrm{Im}(z^{4t}) = \left(\frac{b}{a}\right) \sum_{s=0}^{t-1} \lambda_s B_s\,,$$

and

$$\max_s \left\{\frac{B_s}{A_s}\right\} = \max_s \left\{ \left(\frac{4t-4s}{4s+1}\right) \frac{\left[1 - \frac{(4t-4s-1)(4t-4s-2)}{(4s+2)(4s+3)}\left(\frac{b}{a}\right)^2\right]}{\left[1 - \frac{(4t-4s)(4t-4s-1)}{(4s+1)(4s+2)}\left(\frac{b}{a}\right)^2\right]} \right\}.$$

The argument of the right-hand side is maximized when $s = 0$. So

$$\max_s \left\{\frac{B_s}{A_s}\right\} = \frac{4t}{\alpha}\left[1 - \frac{1}{3}\binom{4t-1}{2}\left(\frac{b}{a}\right)^2\right] \le \frac{4t}{\alpha}\,.$$

Therefore, applying Lemma A.1, we have

$$\left[\frac{\mathrm{Im}(z^{4t})}{\mathrm{Re}(z^{4t})}\right]^2 \le \left[\frac{4t}{\alpha}\right]^2 \left[\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\right]^2.$$

This proves part (iii). Finally, substituting (68) into (67) gives part (iv). ■

References

[1] P. Billingsley. *Probability and measure*. Wiley Series in Probability and Mathematical Statistics. John Wiley & Sons Inc., New York, third edition, 1995. A Wiley-Interscience Publication.

[2] R. Craigen. Signed groups, sequences, and the asymptotic existence of Hadamard matrices. *J. Combin. Theory Ser. A*, 71(2):241–254, 1995.

[3] W. de Launey and D. M. Gordon. A comment on the Hadamard conjecture. *J. Combin. Theory Ser. A*, 95(1):180–184, 2001.

[4] S. W. Graham and I. E. Shparlinski. On RSA moduli with almost half of the bits prescribed. *Discrete Appl. Math.*, 156(16):3150–3154, 2008.

[5] F. Spitzer. *Principles of random walks*. Springer-Verlag, New York, second edition, 1976. Graduate Texts in Mathematics, Vol. 34.

Center for Communication Research, 4320 Westerra Court, San Diego, California 92121-1969

E-mail address: warwickdelauney@earthlink.net

Department of Mathematics, University of Oregon, Eugene, Oregon 97402-1222

E-mail address: dlevin@uoregon.edu

URL: http://www.uoregon.edu/~dlevin